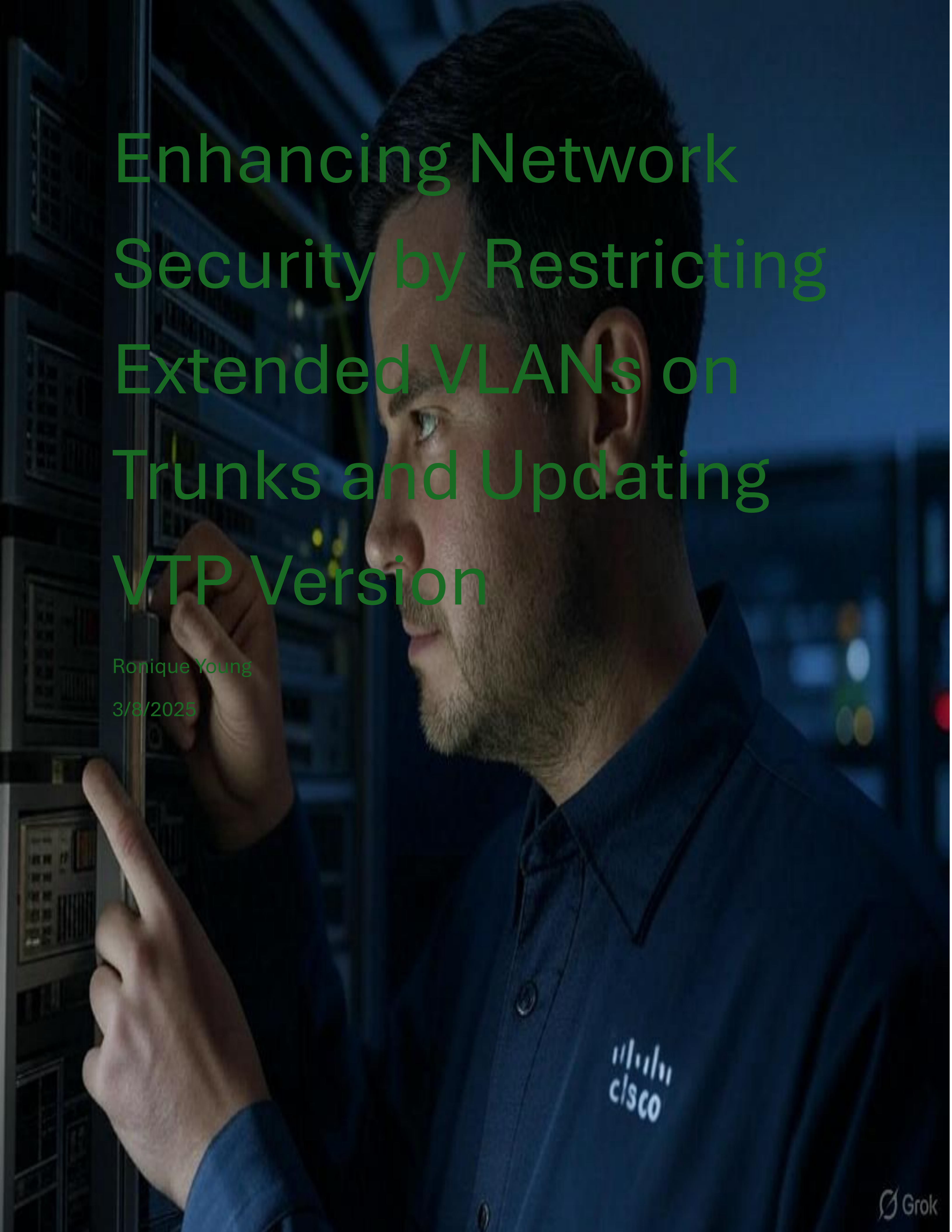
Enhancing Network Security by Restricting Extended VLANs on Trunks and Updating VTP Version

Ronique Young

3/8/2025



Strengthening Network Security with VLAN Trunk Restrictions on a Cisco 2960 Switch

I recently tackled a hands-on lab project using a Cisco Catalyst 2960 switch, focusing on enhancing network security by restricting VLANs on trunk links and updating the VTP version. This exercise sharpened my Cisco configuration skills and taught me how to overcome real-world challenges like the dreaded "Command rejected: Bad VLAN list" error.

What I Did:

VLAN Restriction on Trunks: By default, all VLANs traverse trunk links on a 2960, which can pose security risks. I configured the switchport trunk allowed vlan command to limit traffic to specific VLANs (e.g., 1-5, 10, 20-30). When I hit the "Bad VLAN list" error, I dug into troubleshooting—verifying VLAN existence with show vlan brief, correcting syntax, and ensuring compatibility with the 2960's standard VLAN range (1-1005).

VTP Version Update: I also adjusted the VTP version to streamline VLAN management across the network, reinforcing consistency and control.

Problem-Solving: The 2960's limitations with extended VLANs (1006-4094) required me to adapt my approach, sticking to supported ranges and validating every step with commands like show interfaces trunk.

Key Takeaway:

Precision matters in networking. Overcoming the error involved understanding the switch's capabilities, refining my command syntax, and ensuring only valid VLANs made the cut.

Proud to add this experience to my toolkit—ready to tackle more networking challenges! #Networking #Cisco #CCNA #NetworkSecurity #VLAN #TechSkills

Strengthening
Network Security wi

CLICK HERE TO SEE THE BREAKDOWN IN PKT FILE. RUN THE SHOW RUNNING-CONFIG